IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Previously Presented): In an authentication system in which an authentication server which authenticates a user, a user terminal which transmits a user authentication information, and an application server which provides a service to the user through the user terminal are connected together to enable a communication therebetween through a network, the address based authentication system including:

the authentication server which comprises

authentication means for authenticating a user based on the user authentication information transmitted together with a key information as an authentication request from the user terminal, the key information representing a public key K_{PU} of the user terminal;

an address allocating means for allocating an address to the user terminal for a successful authentication of the user;

generating means for generating information-for-authentication using at least the allocated address;

a ticket issuing means for issuing a ticket containing the allocated address, the key information which is received from the user terminal and the information-for-authentication;

and a ticket transmitting means for transmitting the ticket issued by the ticket issuing means to the user terminal;

the user terminal which has a pair of the public key K_{PU} and a private key K_{SU} and comprises:

transmitting means for transmitting the user authentication information and the key information to the authentication server for purpose of an authentication request;

a ticket reception means for receiving the ticket which contains the allocated address, the key information and the information-for-authentication and which is transmitted from the authentication server;

means for setting up the allocated address contained in the ticket as a source address for each packet which is to be transmitted from the user terminal to the application server;

a first session key generating means for calculating a first session secret key which is shared with the application server, from the private key K_{SU} of the user terminal and a public key K_{PS} of the application server;

a packet cryptographic processing means for processing each packet to be transmitted to the application server by the first session secret key to guarantee that there is no forgery in each packet;

means for transmitting a first packet including the ticket to the application server for establishing a session; and

a service request means for transmitting a second packet requesting the service to the application server through the session;

and the application server which has a pair of the public key K_{PS} and a private key K_{SS} and comprises:

a second session key generating means for calculating a second session secret key which is shared with the user terminal, from the private key K_{SS} of the application server and the public key K_{PU} of the user terminal;

a packet verifying means for confirming whether or not each packet received from the user terminal is forged using the second session secret key;

a ticket memory means for storing the ticket transmitted from the user terminal;

ticket verifying means for verifying the presence or absence of any forgery in the information-for-authentication in the ticket transmitted from the user terminal to determine if

the allocated address contained in the ticket is forged or not and preventing the ticket from being stored in the ticket memory means in the presence of a forgery and further verifying whether or not the key information contained in the ticket in the first packet, which has been verified as not being forged, is the key information representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means;

an address comparison means for determining whether or not the allocated address contained in the ticket which is stored in the ticket memory means coincides with the source address of the second packet which is transmitted from the user terminal through the session; and

a service providing means for transmitting to the user terminal packets which provide the service to the user when a coincidence between the addresses is determined by the address comparison means.

Claim 2 (Cancelled).

Claim 3 (Previously Presented): The authentication system according to Claim 1

the application server further comprising

an address collating means for collating the allocated address in the ticket transmitted from the user terminal against the source address of the first packet which includes the ticket and for preventing the ticket from being stored in the ticket memory means if a coincidence is not found.

Claim 4 (Previously Presented): The authentication system according to Claim 1 in which the authentication server comprises a user identifier allocating means for allocating a

user identifier which corresponds to the authenticated user in response to the authentication request for a successful authentication of the user,

the ticket issuing means being configured to issue the ticket inclusive of the user identifier.

Claim 5 (Previously Presented): The authentication system according Claim 1

in which the authentication information generating means of the authentication server is configured to process the information including the allocated address with a shared secret key which is shared beforehand between the authentication server and the application server,

the ticket verifying means of the application server is configured to further verify the information-for-authentication contained in the ticket using a shared secret key which is beforehand shared between the authentication server and the application server.

Claims 6-14 (Cancelled).

Claim 15 (Previously Presented): An application server in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made to an application server on the basis of the authentication, comprising

a session establishing means for establishing a session with a user terminal in response to a reception of a session establishment request packet containing a ticket from the user terminal, said ticket containing an address allocated by the authentication server to the user terminal, a key information representing a public key K_{PU} of the user terminal and information-for-authentication generated by the authentication server using at least the allocated address;

a ticket memory means in which the ticket transmitted from the user terminal is stored;

an address comparison means to which a source address of a service request packet which is transmitted from the user terminal and received through the established session is input and which determines whether or not the source address coincides with an allocated address of the user terminal contained in the ticket stored in the ticket memory means; and

a service providing means which provides a service to the user terminal when the output of the address comparison means indicates a coincidence,

wherein said session establishing means comprises a ticket verifying means for verifying authenticity of the ticket, which is received from the user terminal for establishing the session, by checking the information-for-authentication contained in the ticket to determine if the allocated address contained in the ticket is forged or not and preventing the ticket from being stored in the ticket memory means when verification is not successful, and further verifying whether or not the key information contained in the ticket in the first packet, which has been verified as not being forged, is the key information representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means.

Claim 16 (Cancelled).

Claim 17 (Previously Presented): The application server according to Claim 15, further comprising

a session key generating means for calculating a session secret key which is shared with the user terminal from a private key of the application server and a public key of the user terminal;

and a packet verifying means for verifying whether or not the session establishment request packet received from the user terminal is forged using the session secret key and for preventing the ticket from being stored in response to a verification output indicating the presence of a forgery.

Claim 18 (Previously Presented): The application server according to Claim 17 in which the ticket verifying means comprises collating means for verifying, when the received session establishment request packet has been verified by the packet verifying means as not forged, whether or not key information contained in the ticket corresponds to the public key of the user terminal which has been used in the calculation of the session secret key.

Claim 19 (Previously Presented): The application server according to Claim 15 in which the ticket verifying means comprises terminal authenticating means to which an authentication purpose shared secret key which is shared with the user terminal and a random number which changes each time a session is established are input and which processes the random number using the authentication purpose shared secret key, collates a result of the processing against a key information in the ticket and verifies the authenticity of the ticket by seeing whether or not a matching between the result of processing and the key information applies.

Claim 20 (Previously Presented): An application server according to Claim 15 in which the ticket verifying means comprises means for verifying whether or not the source address of the received session establishment request packet coincides with the allocated address contained in the ticket within the session establishment request packet and for

preventing the ticket from being stored in response to a detection output which indicates a non-coincidence.

Claims 21-22 (Cancelled).

Claim 23 (Currently Amended): A non-transitory computer readable storage medium having stored thereon an application server program for programming a computer to function as an application server in an authentication system in which an authentication of a user utilizing a user terminal is performed by an authentication server and a request to provide a service is made by the user terminal to the application server on the basis of the authentication, the application server comprising:

a session establishing means for establishing a session with a user terminal in response to a reception of a session establishment request packet containing a ticket from the user terminal, said ticket containing an address allocated by the authentication server to the user terminal, a key information representing a public key K_{PU} of the user terminal and information-for-authentication generated by the authentication server using at least the allocated address;

a ticket memory means in which the ticket transmitted from the user terminal is stored;

an address comparison means to which a source address of a service request packet which is transmitted from the user terminal and received through the established session is input and which determines whether or not the source address coincides with an allocated address of the user terminal contained in the ticket stored in the ticket memory means; and

a service providing means which provides a service to the user terminal when the output of the address comparison means indicates a coincidence,

wherein said session establishing means comprises a ticket verifying means for verifying authenticity of the ticket, which is received from the user terminal for establishing the session, by checking the information-for-authentication contained in the ticket to determine if the allocated address contained in the ticket is forged or not and preventing the ticket from being stored in the ticket memory means when verification is not successful and further verifying whether or not the key information contained in the ticket in the first packet, which has been verified as not being forged, is the key information representing the public key K_{PU} of the user terminal, and if not, prevent the ticket from being stored in the ticket memory means.

Claim 24 (Previously Presented): The system according to Claim 1, in which the authentication server has a secret key and a public key for a digital signature,

and said ticket issuing means comprises:

an authentication information generating means for computing a digital signature on the information including at least the allocated address using the secret key for the digital signature to produce the information for authentication so that the application server can verify the presence or absence of any forgery in the information for authentication in the ticket using the public key of the authentication server.

Claim 25 (Cancelled).